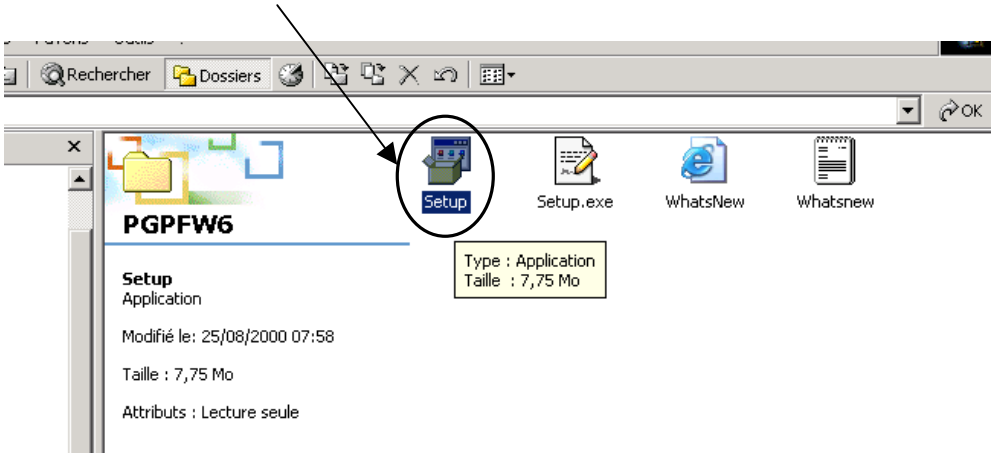
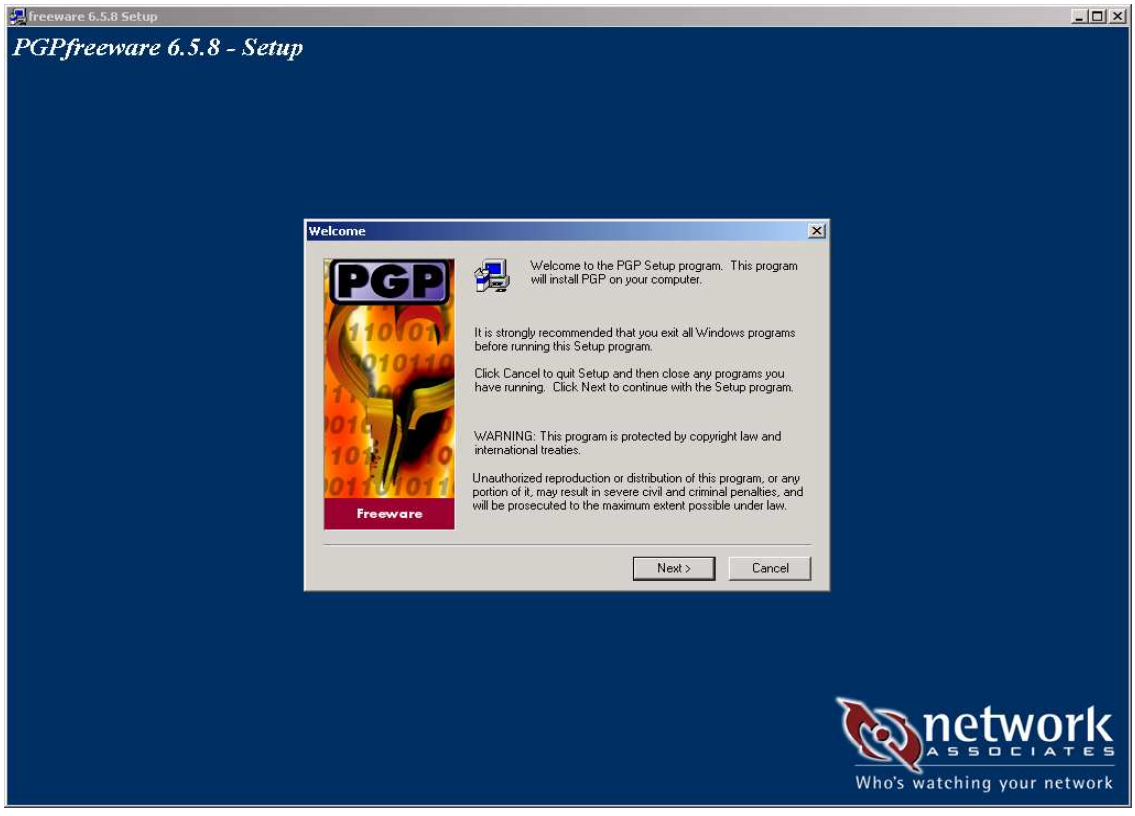
Mode d'emploi pour l'installation et l'utilisation de PGP
Sous Windows 95, 98, 2000, NT et XP

A. PREMIERE ETAPE : Installation de PGP

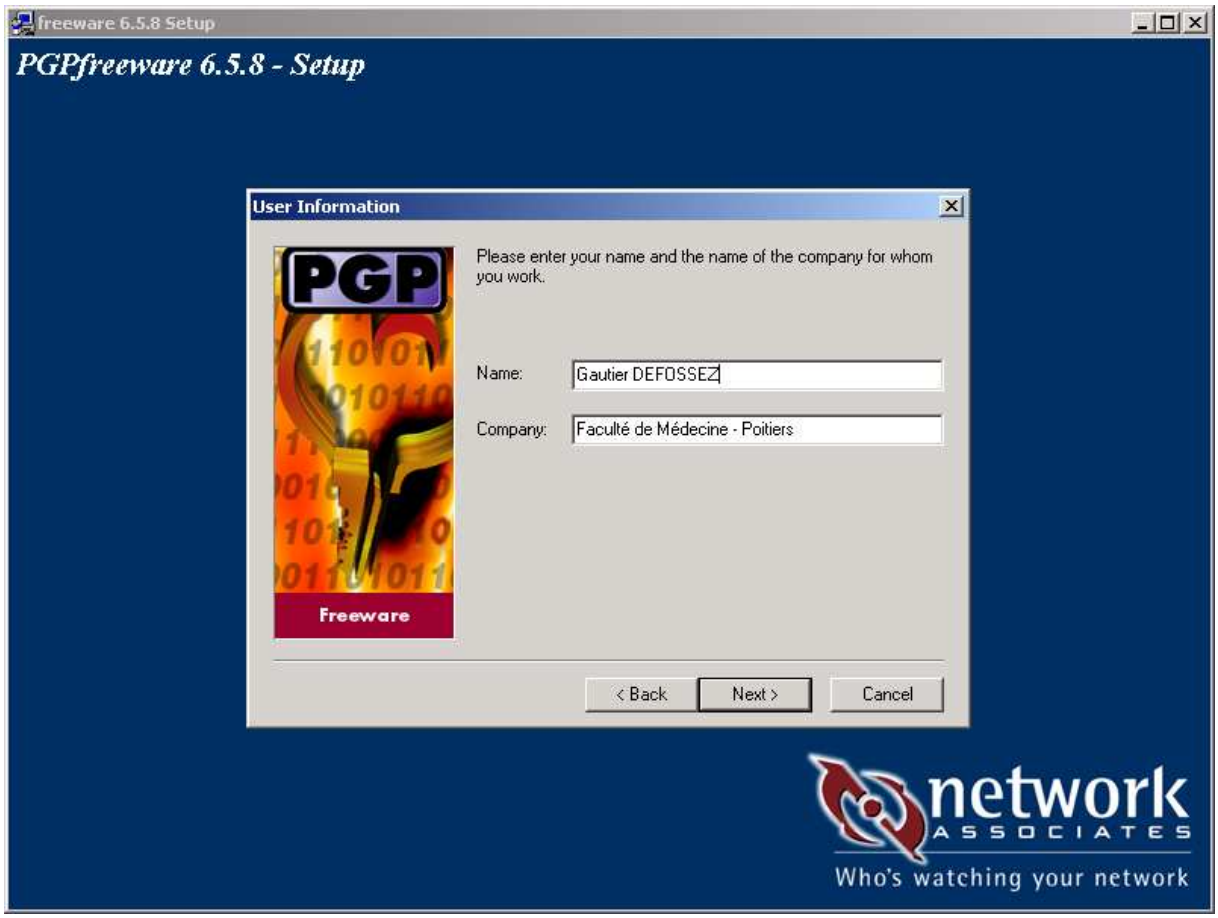
1. Insérez le CD
2. Cliquez sur l'icône (**D :**) du poste de travail pour lancer le disque
3. Ouvrez le dossier « **Version PC** », puis « **PGPFW6** », puis double-cliquez sur l'icône « **Setup** »



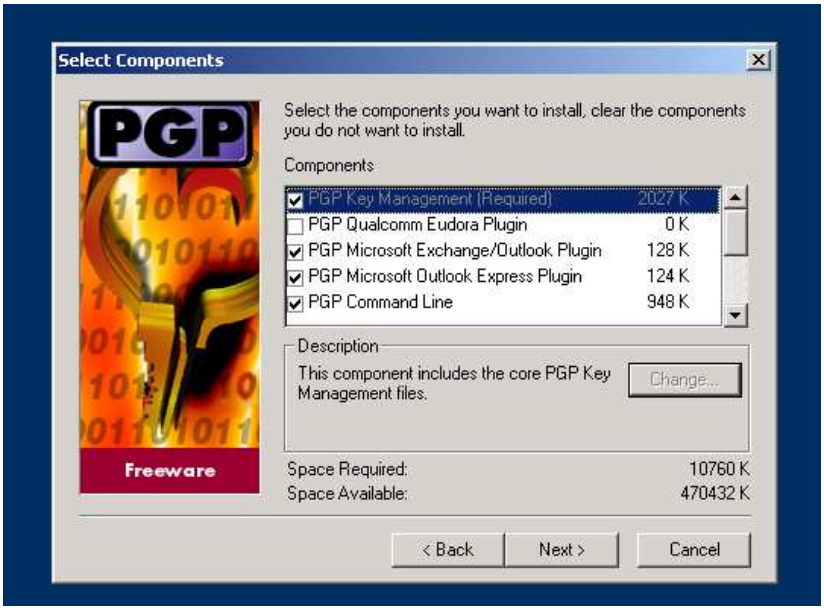
4. PGP lance la procédure d'installation sur votre PC, vous obtenez la page suivante :


freeware 6.5.8 Setup
PGPfreeware 6.5.8 - Setup
Welcome
PGP
Freeware
Welcome to the PGP Setup program. This program will install PGP on your computer.
It is strongly recommended that you exit all Windows programs before running this Setup program.
Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.
WARNING: This program is protected by copyright law and international treaties.
Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.
Next >
Cancel
network
ASSOCIATES
Who's watching your network

5. « **Next** » jusqu'à l'étape où vous êtes amené à remplir les items « **Nom** » et « **Company** » :

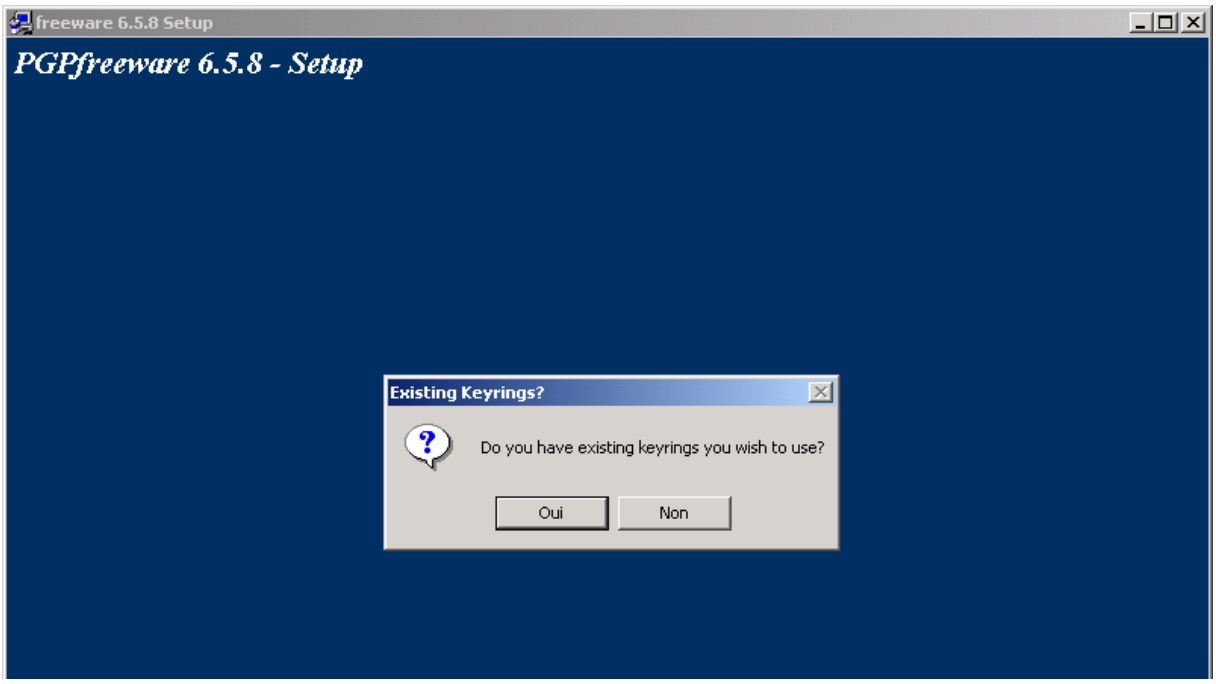


6. « **Next** »
7. Continuez sans changer les paramètres proposés par défaut :


Select Components
Select the components you want to install, clear the components you do not want to install.
Components
PGP Key Management (Required) 2027 K
PGP Qualcomm Eudora Plugin 0 K
PGP Microsoft Exchange/Outlook Plugin 128 K
PGP Microsoft Outlook Express Plugin 124 K
PGP Command Line 948 K
Description
This component includes the core PGP Key Management files.
Change...
Space Required: 10760 K
Space Available: 470432 K
PGP
Freeware
< Back
Next >
Cancel

Nous ne vous conseillons pas l'installation du plugin de messagerie : décochez alors « **PGP Microsoft Exchange/Outlook plugin** »,
Et « **PGP Microsoft Outlook Express Plugin** ».

8. Avez-vous un trousseau de clés existant ? « **NON** »

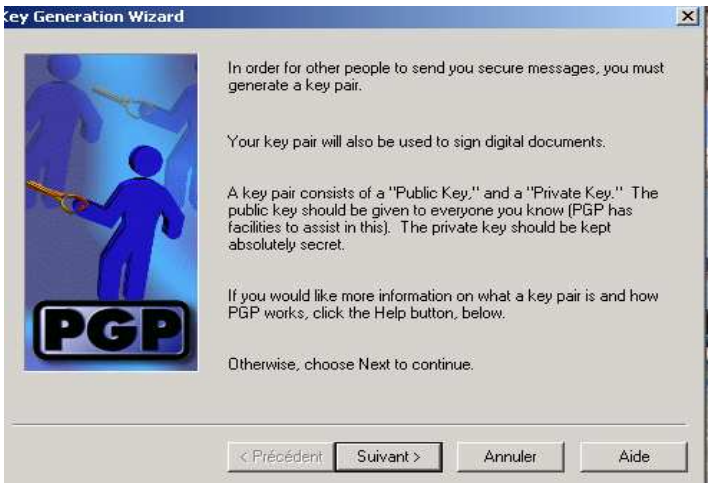


Setup Complete
PGP
Freeware
Setup has finished installing PGP on your computer.
Setup can launch the Read Me file and PGP. Choose the options you want below.
Launch PGPkeys.
Click Finish to complete Setup.
< Back
Finish

La 1ère étape est terminée.

B. SECONDE ETAPE D'INSTALLATION DU LOGICIEL : Création de votre clé publique et de votre clé privée

1. Vous êtes amené à créer votre trousseau de clés, se décomposant en 2 parties :
    a. Une clé publique : que vous allez communiquez à vos correspondants
    b. Une clé privée : qui doit rester strictement confidentielle

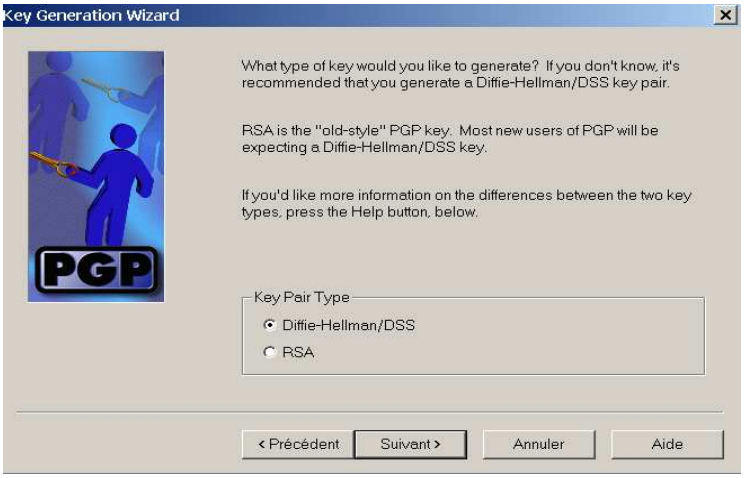

ey Generation Wizard
In order for other people to send you secure messages, you must generate a key pair.
Your key pair will also be used to sign digital documents.
A key pair consists of a "Public Key," and a "Private Key." The public key should be given to everyone you know (PGP has facilities to assist in this). The private key should be kept absolutely secret.
If you would like more information on what a key pair is and how PGP works, click the Help button, below.
Otherwise, choose Next to continue.
< Précédent
Suivant >
Annuler
Aide

2. Entrez votre « **Nom et Prénom** » ou bien le nom de l'organisme/institution, et votre « **Adresse e-mail** » :

ey Generation Wizard
What name and email address should be associated with this key pair?
By listing your name and email address here, you let your correspondents know that the key they are using belongs to you.
Full name:
Gautier DEFOSSEZ
Email address:
gdefossez@hotmail.com
< Précédent
Suivant >
Annuler
Aide

3. « **Suivant** »

4. Optez ensuite pour un type de clé « **Diffie-Hellan/DSS**» (la technologie RSA est utilisée surtout pour les versions de PGP antérieures à 5.0) :
   (Suivez les paramètres affichés par défaut)


Key Generation Wizard
What type of key would you like to generate? If you don't know, it's recommended that you generate a Diffie-Hellman/DSS key pair.
RSA is the "old-style" PGP key. Most new users of PGP will be expecting a Diffie-Hellman/DSS key.
If you'd like more information on the differences between the two key types, press the Help button, below.
Key Pair Type
Diffie-Hellman/DSS
RSA
< Précédent
Suivant >
Annuler
Aide

5. Choisissez après la longueur de la clé qui ne doit pas être excessivement longue (une longueur de « **2048 bits** » est largement suffisante)

Key Generation Wizard
How large a key pair do you wish to generate? As a rule, larger keys are more secure, but slower.
For most applications, 1024 - 2048 bit keys are quite sufficient.
Key Pair Size
1024 bits
1536 bits (1536 Diffie-Hellman/1024 DSS)
2048 bits (2048 Diffie-Hellman/1024 DSS)
3072 bits (3072 Diffie-Hellman/1024 DSS)
Custom (1024 - 4096 bits)
2048
< Précédent
Suivant >
Annuler
Aide

6. Vous pouvez également attribuer une durée de vie à votre jeu de clé si pour une raison ou une autre vous souhaitez en interdire l'utilisation au bout d'un certain temps.

7. Entrez ensuite votre phrase secrète qui doit être connue de vous seul. Plus longue et originale sera la phrase, plus grande sera l'inviolabilité. Mémorisez-la car elle vous sera redemandée plus tard. En cas d'oubli, elle ne pourra pas être récupérée (+++).

Tout caractère compte : accents, majuscules, ponctuations, chiffres (+++).

ey Generation Wizard
Your private key will be protected by a passphrase. It is important that you do not write this passphrase down.
Your passphrase should be at least 8 characters long and should contain non-alphabetic characters.
Passphrase:
Hide Typing
Passphrase Quality :
Confirmation:
PGP
< Précédent
Suivant >
Annuler
Aide

8. « **Suivant** »

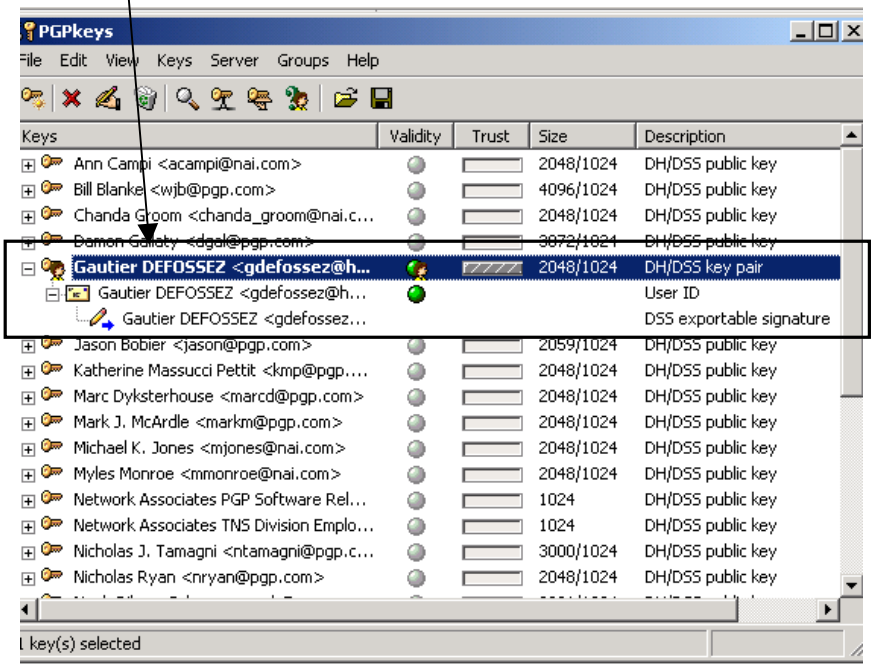
ey Generation Wizard
PGP is now generating your new key pair. On a slow machine, this could take several minutes. Please be patient.
Complete
PGP
< Précédent
Suivant >
Annuler
Aide

9. PGP vous demande ensuite si vous désirez envoyer votre clé publique sur le serveur : « **NON** »

Key Generation Wizard
If you have an Internet connection, we suggest that you send your new public key to the server.
This will make it easy for your correspondents to get your key and communicate with you securely.
If you don't have an Internet connection, or are not connected right now, leave "Send my key to the root server now" unchecked. You can send your key later from within PGPkeys.
Send my key to the root server now
PGP
< Précédent
Suivant >
Annuler
Aide

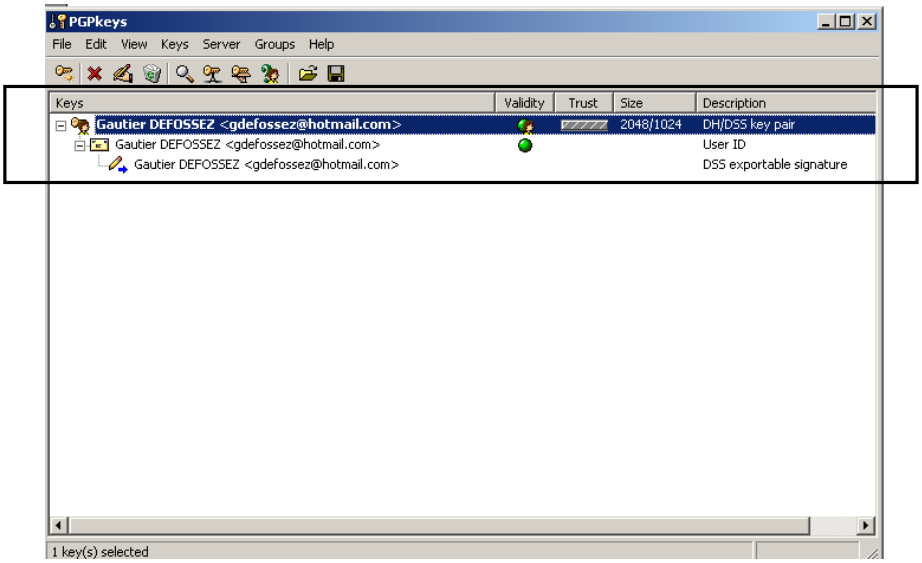
10. Voilà, appuyer enfin sur « **Suivant** », puis sur « **Terminer** ».

11. Alors, apparaît la fenêtre « **PGPkeys** » où figure bien désormais votre propre « répertoire » correspondant à votre clé publique :

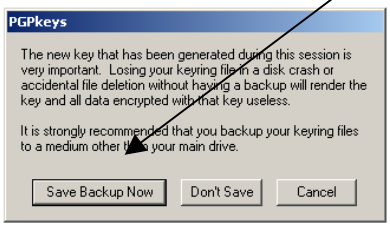

PGPkeys
File Edit View Keys Server Groups Help
Keys
Validity
Trust
Size
Description
Ann Campi <acampi@nai.com> 2048/1024 DH/DSS public key
Bill Blanke <wjb@pgp.com> 4096/1024 DH/DSS public key
Chanda Groom <chanda_groom@nai.c... 2048/1024 DH/DSS public key
Gautier DEFOSSEZ <gdefossez@h... 2048/1024 DH/DSS key pair
Gautier DEFOSSEZ <gdefossez@h... User ID
Gautier DEFOSSEZ <gdefossez... DSS exportable signature
Jason Bobier <jason@pgp.com> 2059/1024 DH/DSS public key
Katherine Massucci Pettit <kmp@pgp.... 2048/1024 DH/DSS public key
Marc Dyksterhouse <marcd@pgp.com> 2048/1024 DH/DSS public key
Mark J. McArdle <markm@pgp.com> 2048/1024 DH/DSS public key
Michael K. Jones <mjones@nai.com> 2048/1024 DH/DSS public key
Myles Monroe <mmonroe@nai.com> 2048/1024 DH/DSS public key
Network Associates PGP Software Rel... 1024 DH/DSS public key
Network Associates TNS Division Emplo... 1024 DH/DSS public key
Nicholas J. Tamagni <ntamagni@pgp.c... 3000/1024 DH/DSS public key
Nicholas Ryan <nryan@pgp.com> 2048/1024 DH/DSS public key
key(s) selected

PGP installe par défaut d'autres nombreuses clés publiques de potentiels destinataires qui ne nous concernent ici en aucun cas. Il est fortement conseillé de les supprimer de « PGPkeys » afin d'y voir nettement plus clair (Clic-droit, puis « **Delete** »).

Vous arrivez alors à cet affichage après les multiples suppressions, ce qui vous permet d'éviter d'éventuelles erreurs de manipulation.



12. Il est important ensuite de sauvegarder votre clé publique et votre clé privée. Cela vous est proposé lorsque vous fermez la fenêtre « **PGPkeys** ». Faites le et enregistrer ces fichiers sur votre disque dur « **Save Backup Now** »
    c. « **Pubring** », puis
    d. « **Secring** »


PGPkeys
The new key that has been generated during this session is very important. Losing your keyring file in a disk crash or accidental file deletion without having a backup will render the key and all data encrypted with that key useless.
It is strongly recommended that you backup your keyring files to a medium other
your main drive.
Save Backup Now
Don't Save
Cancel

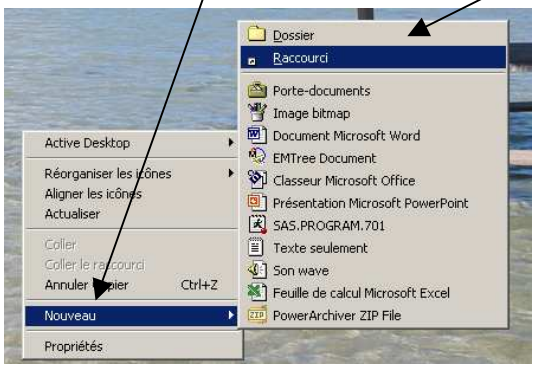
13. Faites ensuite une sauvegarde de ces 2 clés sur un support disquette (à stocker dans un lieu sécurisé), afin de pouvoir les récupérer en cas de panne système.

14. Voilà, vos clés ont été crées, elles vous sont propres.

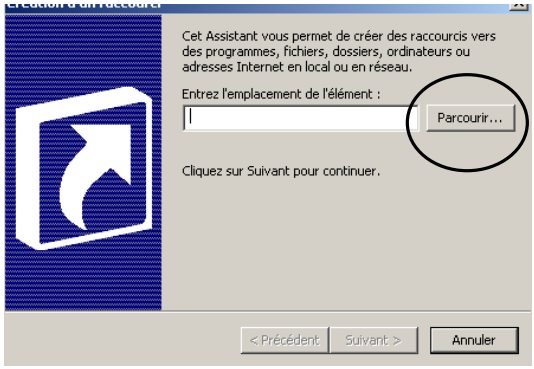
C. TROISIEME ETAPE DE L'INSTALLATION : Création des raccourcis et import de la clé « Registre des Cancers »

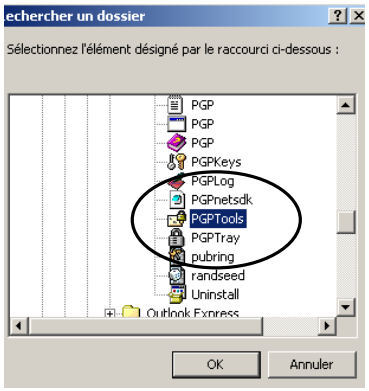
1. Disposez le raccourci sur le bureau de la façon suivante :

- Clic-droit sur le bureau, « **Nouveau** », puis « **Raccourci** »,



- Allez chercher l'icône « **PGPtools** » en cliquant sur « **Parcourir** » et suivez le chemin suivant « **C:\Program Files\Network Associates\PGPNT** » :

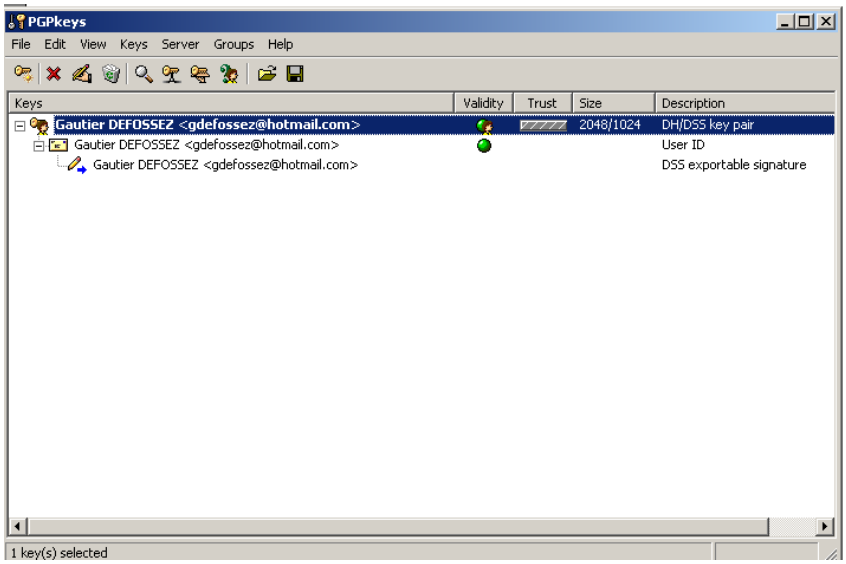

Cet Assistant vous permet de créer des raccourcis vers des programmes, fichiers, dossiers, ordinateurs ou adresses Internet en local ou en réseau.
Entrez l'emplacement de l'élément :
Parcourir...
Cliquez sur Suivant pour continuer.
< Précédent
Suivant >
Annuler



- « **Ok** », « **Suivant** » et enfin « **Terminer** ».

2. Pour lancer PGP, il vous suffit alors de double-cliquez sur l'icône que vous venez d'installer sur votre bureau « **PGPtools** », pour voir apparaître la barre d'outils nécessaire à l'utilisation de PGP.

Faites apparaître la fenêtre « **PGPkeys** » en cliquant sur le bouton le plus à Gauche.

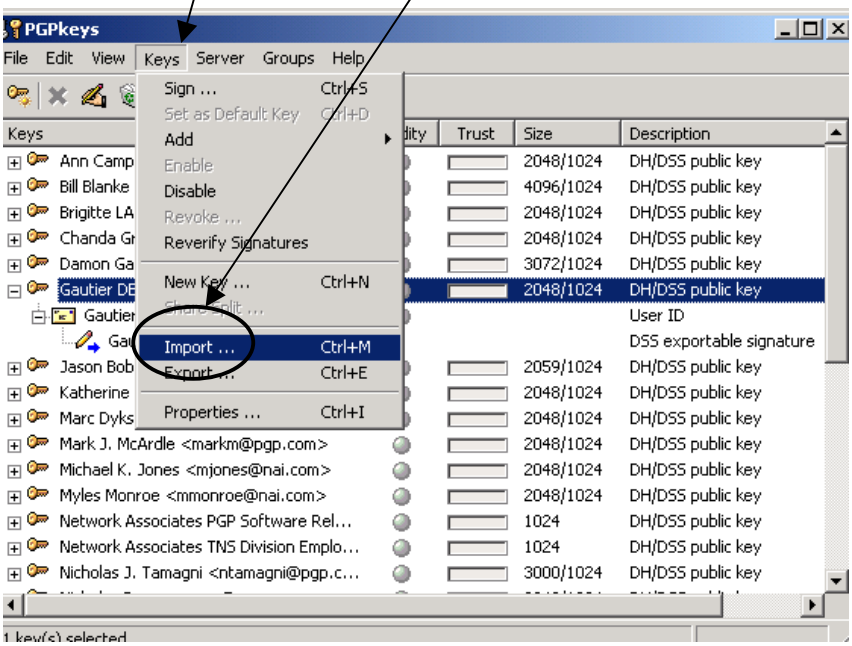


3. L'étape suivante consiste à importer la clé publique **« Registre des Cancers »** jointe sur le CD d'installation du logiciel, indispensable à l'échange de fichiers cryptés entre vous et le registre.

Pour mieux comprendre :
L'échange de fichiers entre 2 personnes « **X** » et « **Y** » nécessite la conjonction des 2 clés publiques (+++).
Si « X » désire transmettre un fichier crypté à « Y », il devra alors effectuer le cryptage du fichier à partir de la clé publique de « Y » , d'où l'importance d'importer les clés publiques de vos correspondants, ici le **Registre des Cancers**.
De même, « Y » ne pourra décrypter le fichier de « X » que s'il a importer auparavant la clé publique de « X ».
La clé privée sert essentiellement au moment de l'ouverture du fichier crypté, en passant par la demande de votre phrase secrète.

Ainsi, il vous faut désormais importer la « Clé Publique Registre des Cancers».

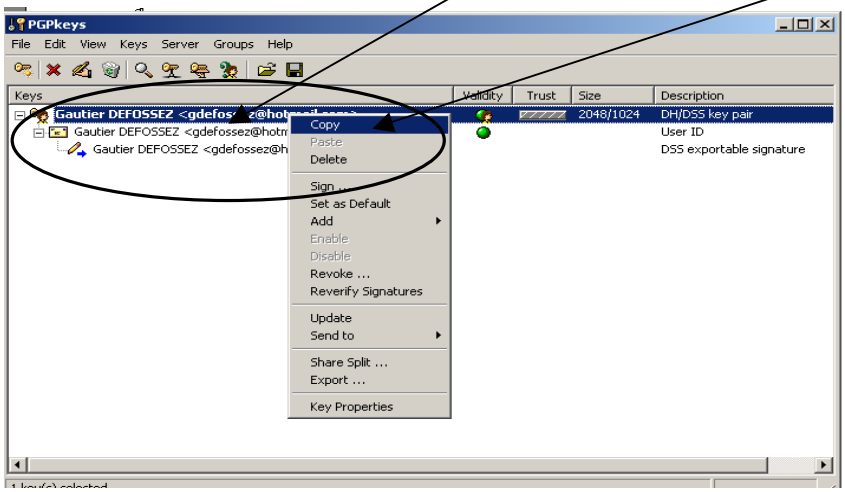
- Cliquez sur l'icône « **Keys** », puis « **Import** » afin d'enregistrer la clé publique Registre des Cancers dans votre répertoire.


PGPkeys
File Edit View Keys Server Groups Help
Sign ... Ctrl+S
Set as Default Key Ctrl+D
Add
Enable
Disable
Revoke ...
Reverify Signatures
New Key ... Ctrl+N
Import ... Ctrl+M
Export ... Ctrl+E
Properties ... Ctrl+I
Keys
Trust
Size
Description
Ann Camp 2048/1024 DH/DSS public key
Bill Blanke 4096/1024 DH/DSS public key
Brigitte LA 2048/1024 DH/DSS public key
Chanda Gr 2048/1024 DH/DSS public key
Damon Ga 3072/1024 DH/DSS public key
Gautier DE 2048/1024 DH/DSS public key
Gautier User ID
Ga DSS exportable signature
Jason Bob 2059/1024 DH/DSS public key
Katherine 2048/1024 DH/DSS public key
Marc Dyks 2048/1024 DH/DSS public key
Mark J. McArdle <markm@pgp.com> 2048/1024 DH/DSS public key
Michael K. Jones <mjones@nai.com> 2048/1024 DH/DSS public key
Myles Monroe <mmonroe@nai.com> 2048/1024 DH/DSS public key
Network Associates PGP Software Rel... 1024 DH/DSS public key
Network Associates TNS Division Emplo... 1024 DH/DSS public key
Nicholas J. Tamagni <ntamagni@pgp.c... 3000/1024 DH/DSS public key
1 key(s) selected

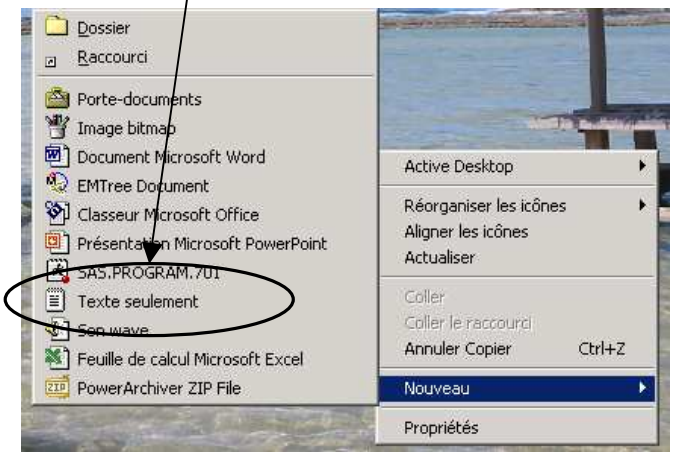
- Sélectionner le fichier « **Clé Publique Registre des Cancers**» présent sur le CD en format texte, puis « **ouvrir** », et enfin « **Import** ».

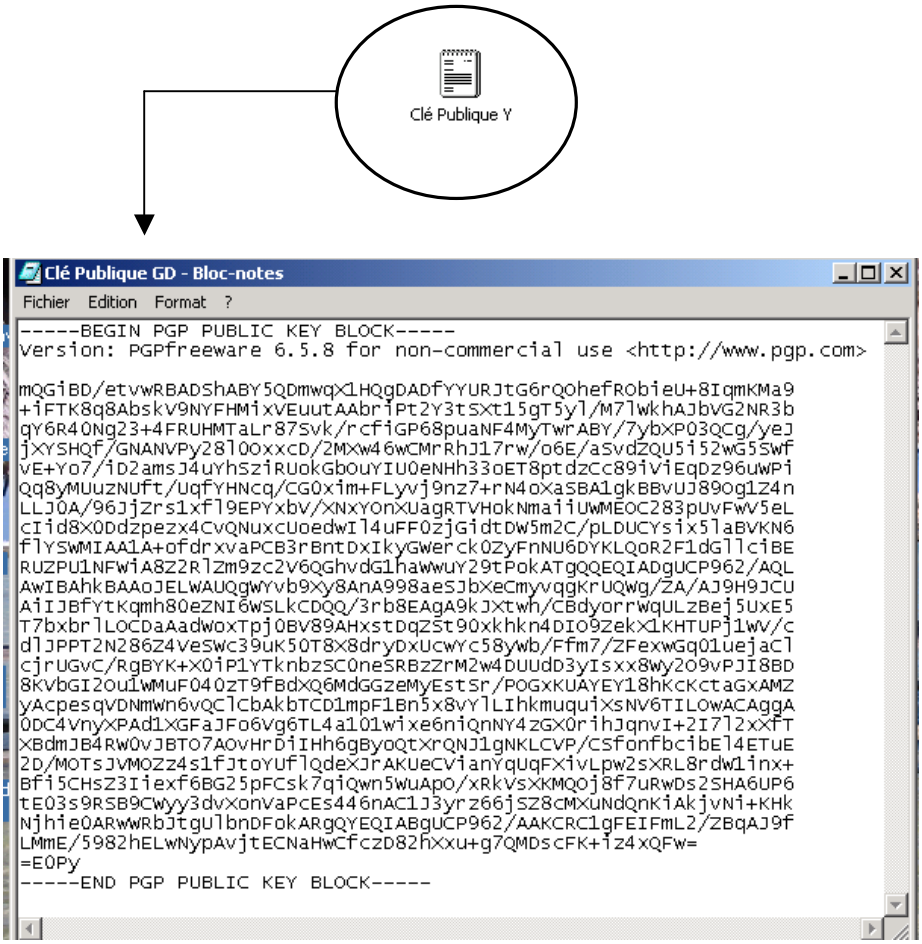
4. Ensuite, envoyez « votre » clé publique au Registre des cancers, étape indispensable à l'échange de fichiers cryptés entre vous et le registre. Pour ceci, procédez de la manière suivante :

✓ Effectuez un clic-droit sur votre « **Nom Prénom** », puis clic sur « **Copy** »



✓ Positionnez vous alors sur le bureau et effectuez de nouveau un clic-droit, « **Nouveau** », « **Texte seulement** » (renommez-le), ouvrez-le et aller y **copier** votre clé publique (clic-droit, « Copy »).





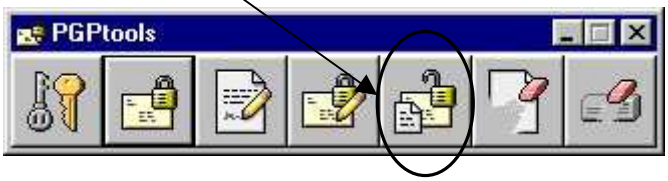
- ✓ Enregistrez les modifications, puis fermez le fichier texte.
- ✓ Envoyez le au registre par messagerie électronique, qui l'importera à son tour dans son répertoire pour échanger ainsi des fichiers cryptés.

  Mail : gautier.defossez@univ-poitiers.fr

D. UTILISATION DE PGP :

✓ POUR DECRYPTER UN FICHIER :

1. Pour décrypter un fichier envoyé par le Registre, lancez « **PGPtools** » et cliquez sur l'icône « **Decrypt/Verify** »



2. Sélectionnez alors le fichier à décrypter (que vous aurez préalablement enregistrer sur le disque dur de votre système à partir de votre messagerie), puis entrez votre phrase secrète.

3. Le fichier décrypté apparaît alors dans le même répertoire que le fichier crypté. Voilà, vous pouvez maintenant l'ouvrir normalement.

✓ POUR CRYPTER UN FICHIER :

1. Pour crypter un message destiné au Registre, cliquez maintenant sur l'icône « **Encrypt** » de la barre d'outils « **PGPtools** », puis allez chercher par l'intermédiaire de l'Explorateur Windows le fichier qui vous intéresse.

2. Allez chercher la clé publique de votre destinataire, ici le Registre (qui seul pourra ouvrir le fichier crypté à partir de sa clé privée !) en double-cliquant sur son nom, puis sur « **ok** » :

3. PGP vous demande ensuite l'emplacement de l'enregistrement sur le disque dur de votre fichier crypté.

4. Voilà, vous pouvez désormais l'envoyer par messagerie, en tant que pièces jointes.

MERCI BEAUCOUP POUR VOTRE PATIENCE